APPENDIX I

1. (amended) An authentication system made up by a portable terminal and an authentication device provided independently of said portable terminal for communication with said portable terminal, said authentication system comprising:

first identification information storage means having the first identification information pre-stored therein for discriminating said portable terminal;

operating means for inputting the second identification information associated with said first identification information;

encryption means for encrypting the second identification information input by said operating means based on the preset encryption key generating information; and

first communication means for communication with said authentication device;

said authentication device including

second identification information storage means for storage of the first identification information and the second identification information therein;

encryption key generating information generating means for generating said encryption key generating information;

second communication means for communication with said portable terminal, ~~;~~ and

comparator authentication means for comparing and authenticating the second identification information encrypted by said encryption means based on said encryption key generating information, ~~;~~ wherein

said portable terminal encrypts the second identification information input from said operating means, based on said encryption key generating information received from said authentication device, the ~~so~~ so-encrypted second identification information is transmitted through said first communication means to said authentication device, and wherein, in said authentication device, and the encrypted second identification information received through said second communication means and the second identification information stored by said second identification information storage means are compared to each other based on said encryption key generating information by way of performing the authentication.

2. (amended) The authentication system according to claim 1 wherein said authentication device includes

decoding means for decoding the second identification information encrypted by said encrypting means based on said encryption key generating information, ~~;~~

said authentication device decoding the received encrypted second identification information based on said encryption key generating information, ~~,~~ said authentication device comparing the decoded second identification information to the second identification information stored in said second identification information storage means, by way of performing the authentication.

3. (amended) The authentication system according to claim 2, wherein said encryption key generating information is a random number made up by a preset number of letters, and wherein said second identification information is a password of a service user made up of a preset letter string or a preset string of numerical figures,

4. (amended) The authentication system according to claim 3 for authenticating a service user~~,~~ to whom preset services are offered from a service provider~~,~~ in a credit sale system, an inter-account instant payment system and in ~~an~~ E-commerce~~,~~ carried out over a preset network, wherein

said portable terminal is a card-shaped portable terminal issued by said service provider to said service user, ~~,~~

said authentication device being contained in a host computer in which said service provider authenticates the use information by said service user, ~~,~~ and

said service user being authenticated by said authentication device authenticating said portable terminal and that said service user is a true owner of the portable terminal.

5. (amended) The authentication system according to claim 4, wherein said first and second communication means are wired or wireless communication means.

6. (amended) The authentication system according to claim 4, wherein said portable terminal includes transient storage means in which the second identification information is stored transiently.

7. (amended) The authentication system according to claim 4, wherein said transient storage means stores the second identification information input by said operating means until authentication of said portable terminal by said authentication device.

8. (amended) The authentication system according to claim 4, wherein said second identification information stored in said transient storage means is erased every preset time interval.

9. (amended) The authentication system according to claim 4, wherein said operating means in said portable terminal includes means for erasing the second

identification information stored in said transient storage means.

10. (amended) The authentication system according to claim 4, wherein said operating means in said portable terminal includes a plurality of input units for letters or numerical figures for inputting said second identification information, and wherein the arraying positions of said letter input units are variable.

11. (amended) The authentication system according to claim 10, wherein the arraying positions of said letter inputting units are varied prior to the inputting of said second identification information.

12. (amended) The authentication system according to claim 10, wherein said operating means in said portable terminal includes a display unit for displaying letters and a selection unit for selecting the letters displayed on said display unit, and wherein the second identification information input by said operating means is made up by a string of letters selected by said selection unit from among plural letters sequentially displayed on said display unit.

13. (amended) An authentication method in which a portable terminal is authenticated by an authentication

device provided independently of said portable terminal, said method comprising:

an operating step of inputting the second identification information associated with a first identification information for discriminating said portable terminal, pre-stored in said first identification information storage means;

an encryption key generating information generating step of generating the encryption key generating information;

an encrypting step of encrypting the second identification information input at said operating step, based on the encryption key generating information generated in said encryption key generating information generating step; and

a comparison authentication step of comparing the second identification information encrypted in said encrypting step to said encryption key generating information by way of performing the authentication.

14. (amended) The authentication method according to claim 13 further comprising:

a decoding step of decoding the second identification information, encrypted in said encrypting step, based on said encryption key generating information;

the encrypted second identification information being decoded in said decoding step based on said encryption key generating information, ~~+~~ and the decoded second identification information being compared to the second identification information stored in said second identification information storage means by way of performing the authentication.

15. (amended) The authentication method according to claim 14, wherein the encryption key generating information is a random number comprised of a preset number of letters.

16. (amended) The authentication method according to claim 15 for authenticating a service user, ~~,~~ to whom preset services are offered from a service provider, ~~,~~ in a credit sale system, an inter-account instant payment system and in ~~an~~ E-commerce, ~~,~~ carried out over a preset network, wherein

said portable terminal is a card-shaped portable terminal issued by said service provider to said service user, ~~,+~~

said authentication device being an authentication device contained in a host computer in which said service provider authenticates the use information by said service user, ~~,+~~ and

said service user being authenticated by said authentication device authenticating said portable terminal

and that said service user is a true owner of the portable terminal.

17. (amended) The authentication method accordig to claim 16, wherein said portable terminal and the authentication device are interconnected by wired or wireless communication means.

18. (amended) The authentication method according to claim 16, wherein said portable terminal includes a transient storage step of transiently storing the second identification information.

19. (amended) The authentication method according to claim 16, wherein said transient storage step stores the second identification information input in said operating step until authentication of said portable terminal by said authentication device.

20. (amended) The authentication method according to claim 16, wherein said second identification information stored in said transient storage step is erased every preset time interval.

21. (amended) The authentication method according to claim 16, wherein said operating step includes a step of erasing the second identification information stored in said transient storage step.

22. (amended) The authentication method according to claim 16, wherein said operating step includes a letter inputting step of inputting said second identification information, and wherein the second identification information is input in said letter inputting step via a plurality of letter inputting units the arraying positions of which are variable.

23. (amended) The authentication method according to claim 22, wherein the arraying positions of said plural letters in said letter inputting step are varied prior to inputting of said second identification information.

24. (amended) The authentication method according to claim 22, wherein said operating step includes a display step of displaying letters and a selection step of selecting the letters displayed in said display step, and wherein the second identification information input by said operating step is made up by a string of letters selected in said selection step from among plural letters sequentially displayed in said display step.

25. (amended) An encryption key inputting device in which a string of a preset number of letters comprised of a combination of letters included in a preset group of letters is a letter string for authentication, said device comprising:

display means for irregularly displaying the letters included in said preset group of letters, ~~,~~ and selection means for selecting said letter string for authentication from among the letters irregularly displayed on said display means.

26. (amended) The encryption key inputting device according to claim 25, wherein said preset group of letters is ten numerical figures from 0 to 9.

27. (amended) The encryption key inputting device according to claim 25, wherein said display means irregularly displays said numerical figures in optional positions in said display means.

28. (amended) The encryption key inputting device according to claim 25, wherein said display means displays said numerical figures one-by-one in an irregular sequence.

29. (amended) The encryption key inputting device according to claim 25, wherein said display means displays the pre-entered numerical figures ~~of~~ from 0 to 9 or the vicinity thereof by emitting light thereat to indicate respective numerical figures.

30. (amended) An encryption key inputting method in which a string of a preset number of letters comprised of a combination of letters included in a preset group of

letters is a letter string for authentication, said method comprising:

a displaying step of irregularly displaying the letters included in said preset group of letters; and

a selection step of selecting said letter string for authentication from among the letters irregularly displayed in said display step.

31. (amended) The encryption key inputting method according to claim 30, wherein said preset group of letters is ten numerical figures from 0 to 9.

32. (amended) The encryption key inputting method according to claim 30, wherein said display step irregularly displays said numerical figures in optional positions in said display step.

33. (amended) The encryption key inputting method according to claim 30, wherein said display step displays said numerical figures one-by-one in an irregular sequence.

34. (amended) The encryption key inputting method according to claim 30, wherein said display step displays the pre-entered numerical figures ~~of~~ from 0 to 9 or the vicinity thereof by emitting light thereat to indicate respective numerical figures.

35. (amended) A portable terminal authenticated by an authentication device, comprising:

first identification information storage means having the first identification information for discriminating said portable terminal pre-stored therein,

operating means for inputting the second dentification information associated with said first identification information,

communication means for communication with said authentication device, and

encrypting means for encrypting the second identification information input by said operating means based on preset encryption key generating information sent over said communication means from said authentication device.

36. (amended) The portable terminal according to claim 35, wherein said encryption key generating information is a preset number of random numbers.

37. (amended) The portable terminal according to claim 35, wherein the portable terminal is issued to said service user by a service provider to offer preset services for said service user in a credit sale system, an inter-account instant payment system and ~~in an~~ E-commerce, carried out over a preset network, and is in the form of a card.

38. (amended) The portable terminal according to claim 37, wherein said communication means are wired or wireless communication means.

39. (amended) The portable terminal according to claim 37, wherein said portable terminal includes transient storage means in which the second identification information is stored transiently.

40. (amended) The portable terminal according to claim 39, wherein said transient storage means stores the second identification information input by said operating means until authentication of said portable terminal by said authentication device.

41. (amended) The portable terminal according to claim 39, wherein said second identification information stored in said transient storage means is erased every preset time interval.

42. (amended) The portable terminal according to claim 39, wherein said operating means in said portable terminal includes means for erasing the second identification information stored in said transient storage means.

43. (amended) The portable terminal according to claim 37, wherein said operating means includes a plurality of letter inputting means for inputting said second

identification information, and wherein the arraying positions of said letter inputting units are variable.

44. (amended) The portable terminal according to claim 43, wherein the arraying positions of said plural letters in said letter inputting means are varied prior to the inputting of said second identification information.

45. (amended) The portable terminal according to claim 43, wherein said operating means includes a display unit for displaying letters and a selection unit for selecting the letters displayed in said display unit, and wherein the second identification information input by said operating means is made up by a string of letters selected in said selection unit from among plural letters sequentially displayed on said display unit.

46. (amended) An authentication system made up by a portable terminal and an authentication device provided independently of said portable terminal for communication with said portable terminal, said authentication system comprising:

first identification information storage means having the first identification information pre-stored therein for discriminating said portable terminal;

operating means including display means for irregularly displaying letters included in a group of

letters and selection means for selecting the letters making up the second identification information from among the letters irregularly displayed on said display means, said operating means inputting the second identification information associated with said first identification information,

encryption means for encrypting the second identification information input by said operating means based on the preset encryption key generating information, and

first communication means for communication with said authentication device,

said authentication device including

second identification information storage means having the first identification information and the second identification information stored therein,

encryption key generating information generating means for generating said encryption key generating information,

second communication means for communication with said portable terminal, and

comparator authentication means for comparing the second identification information encrypted by said encryption means to said encryption key generating information by way of authentication, wherein

said portable terminal encrypts the second identification information input from said operating means, based on said encryption key generating information received from said authentication device through said first communication means, and the so encrypted second identification information is transmitted through said first communication means to said authentication device, and wherein, in said authentication device, the encrypted second identification information received through said second communication means and the second identification information stored by said second identification information storage means are compared to each other based on said encryption key generating information by way of performing the authentication.

APPENDIX II

ABSTRACT

An authentication system in which unauthorized acquisition of the private information ~~by~~ of a third party in the course of authentication of a user by a service provider is rendered difficult. In an authentication system in which a card 10 and a host computer 20 are interconnected over a connection line 30, the card 10 includes a memory for ID 11 for storing the card ID, an input unit 12 fed with a secret identification number, a card side interface 13 connected to the host computer 20, an information encryption unit 14 for generating the information for authentication by mixing a random number~~,~~ sent from the host computer 20 and having a unique value each time it is sent~~,~~ with the secret identification number of the card~~,~~ and ~~by~~ encoding the resulting mixed signal, and a transient storage unit 15 for transiently storing the information for authentication as obtained by the information encryption unit 14.